Secure and Strong Mobile cloud Authentication

Qassim Bani Hani , Julius Dichter
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

Mobile cloud computing has dual benefits that include cloud computing and mobile computing. In mobile cloud computing data storage and data processing take place outside the mobile device. As a result, there is a high chance of a security attack. The attacker may easily get access to our sensitive data. Due to this the malicious user may see or modify our data. To overcome this problem, we need to store our data in the cloud where it will be secured. In this paper, we propose a secure and strong authentication (SSA) process that stores the key at different cloud servers. This process provides strong authentication. Greencloud is used to validate the process. The results confirm that our proposed SSA protects the mobile cloud computing from malicious activities.

Introduction

Generally, the mobile computing architecture consists of "Radio Sub System (RSS), Network Sub System (NSS) and Operating Sub System. In RSS all the mobile stations are connected to base station sub system. In NSS all the base station controllers are connected to mobile controller. The operations Support Systems (OSS) consists of an authentication center that controls the NSS and RSS. Risks on mobile cloud computing include privacy, integrity, and authentication attacks.

In mobile computing the large data is stored in the cloud servers. Here, we have to consider three factors: the mobile cloud should securely store the data, the data should be transferred correctly and finally the data should be received by the correct user

Managing these three factors is a cumbersome process. Thus, transferring data from the cloud to mobile devices face the problem of malicious users that can exploit the confidential and sensitive data. Limiting the access of adversary to mobile cloud computing, there is need of strong authentication process. Here, we propose a secure strong authentication process based on One-time password (OTP). In this process, the user information is forwarded to cloud owner prior to accessing the mobile cloud that helps to identify the authenticity of the user. If the mobile cloud user is authenticated then OTP is sent for accessing the cloud, otherwise the access is denied. Our proposed approach protects the mobile devices against authentication attacks. In our proposed approach, we store the key on different mobile clouds, so it is difficult to the attacker to break the key. This process secures the data in the cloud servers by providing strong authentication

Proposed strong Secure and authentication process

In order to keep the data more secure, we designed a secure and strong authentication process. For strong authentication we first have to make a strong key, for which we use the SSA algorithm to encrypt the data. Only the cloud owner is aware of the encryption algorithm.

After encryption, the key is stored on different cloud servers by splitting, so when the attacker wants to break the key it is very difficult to get each piece of the key from the different cloud servers. Even if the attacker gets all the pieces of the key then it is not capable to understand the pattern of the keys.

Algorithm 1: Secure and strong authentication process

1. Initialize: (U_i= user, O_i = owner, A_s = authentication server, C_s = cloud server)
2. User requests => owner
3. Owner sends => authentication server
4. Authentication server gives token => user
5. User maps token to cloud server
6. Cloud server access
7. Key $_1$ =>C_{s1}
8. Key $_2$ =>C_{s2}
9. Key $_3$ =>C_{s3}
10. Get access to the resources

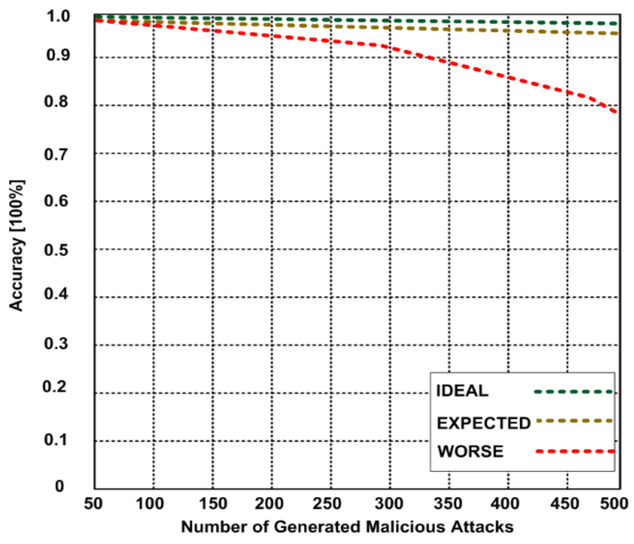
In this strong authentication process when a user wants to get access to the data, she has to get the key from the owner. The process to get the key is explained in algorithm 1.

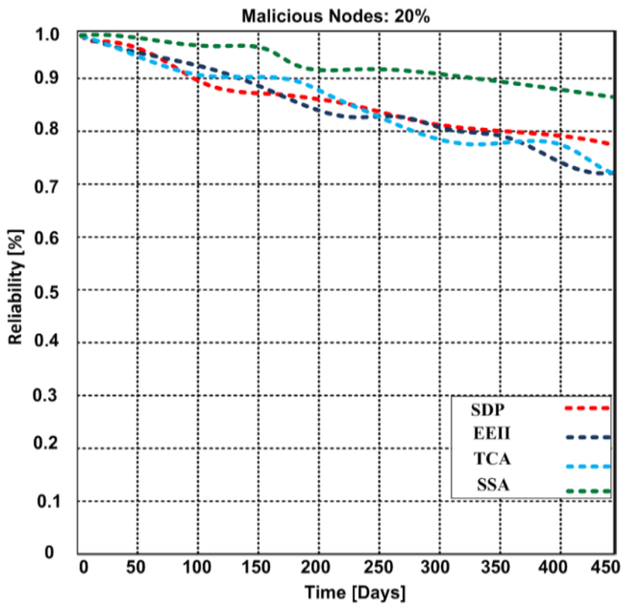
Firstly, the user requests the cloud owner to use the data present in the cloud server. Then the cloud owner collects the owner data and sends that to the authentication server that checks whether the user is legitimate or not and sends token to the user, if the user is legitimate. Then the user sends the token to the cloud server the cloud server checks the information and generates key for the user, if the user is not the correct person then the server alerts the owner that some attacker is trying to get access to his sensitive data and terminates the unsuccessful attack. When the key from the user matches to the cloud server then it provides access to the user to use the resources. The entire secure authentication process is depicted in Figure 1.

Experimental Results

To show the effectiveness of the proposed secure and strong authentication approach, we tested the SSA in different scenarios. We generated data center supported scenarios. The network size consists of 1200 X 1200 square meters. We used 1860 chassis switches, 1456 line cards and 46 ports in the core layer. In the aggregation layer 214 chassis switches, 123 line cards and 48 ports were used. The data center is used by maximum 13200 users.

Accuracy and reliability are considered as the basic criteria to measure the quality of any proposed model. These measures are also used as obvious measures for prediction. We show the accuracy and reliability of our model below:





Conclusion

In this paper, a secure and strong authentication algorithm is proposed for authenticating a mobile user in the mobile cloud computing environment. In our proposed algorithm, a secret encryption key is made split and stored on different cloud servers. The SSA protects the mobile cloud users against the malicious activities. It can provide strong and secure authentication protecting against malicious users and any generated attacks. The SSA also helps maintain the privacy of mobile cloud users. In the future, we will extend our SSA algorithm and determine its computational complexity in mobile cloud environment.